GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Health, Education, and
Human Services Division

B-286077

August 21, 2000

The Honorable Steve Horn
Chairman, Subcommittee on Government Management, Information, and Technology
Committee on Government Reform
House of Representatives

Subject: Responses to Questions From May 18th Hearing on Uses of Social Security Numbers

Dear Mr. Chairman:

I would like to thank you for the opportunity to testify at the May 18, 2000, hearing on the uses of Social Security Numbers (SSN). At that hearing, I agreed to get back to you on two questions, and today I am providing you with the information we were able to obtain.

First, you asked what problems are caused when necessary SSNs are not included on tax forms submitted to the Internal Revenue Service (IRS). When this occurs, IRS cannot link the taxpayer's information to other relevant past or future records. Basically, if IRS receives a tax return that does not contain the SSN of the primary taxpayer (the one filing the return),[1] the return is not to be processed until an SSN is obtained, generally by corresponding with the taxpayer. Also, if the return does not contain an SSN for a dependent child or a child for whom the taxpayer is claiming the Earned Income Tax Credit, the return is processed, but the taxpayer is not to be allowed a dependent exemption or any deduction or credit associated with the dependent, such as the credit for child and dependent care expenses and the child tax credit. If taxpayers later provide the missing SSNs, they are to be allowed the dependent exemption and any credit associated with the SSN. When SSNs are missing from information returns, such as forms 1099 for interest income and dividends, these are sent back to the payer.

Second, you asked what actions federal agencies are taking in the area of using biometrics to identify individuals. Biometric recognition provides automated methods of identifying a person on the basis of a physiological or behavioral characteristic. Various human characteristics are used for biometric recognition, including

[1]On a joint return the primary taxpayer is the one whose name is first on the return.

fingerprints, speech, face, retina, iris, handwritten signature, hand geometry, and wrist veins. Biometric recognition can be used for both identification and verification. For instance, biometric recognition can be used to identify an individual by searching a database consisting of an entire enrolled population for a match. A biometric system can also be used to verify, or authenticate, a person's claimed identity by determining whether it matches his or her previously enrolled pattern. Possible uses also include control of physical access to restricted areas, network security, and computer security. We found a number of examples of biometrics in use or under consideration in the federal government.

- The Immigration and Naturalization Service (INS) is using biometric recognition to provide prompt admission for authorized travelers to the United States by allowing them to bypass the personal interview/inspection part of the entry process. Specifically, INS uses hand geometry to verify the identity of the traveler at an automated inspection station. Travelers arriving at a port of entry proceed to an INS Passenger Accelerated Service System (INSPASS) kiosk, where they insert a card in a machine similar to an automated bank teller machine. They respond to messages (such as "enter flight number") on the touch-screen display and place their hand in a hand geometry reader.[2] The kiosk software automatically compares the live scan of the traveler's hand geometry to the image captured at enrollment. If the traveler's identity is validated, he or she can proceed. If not, the traveler is instructed to see an Immigration Inspector. The INSPASS system has been installed at international airports at Los Angeles, Miami, Newark, New York (John F. Kennedy Airport), and San Francisco.

- The INS also uses Port Passenger Accelerated Service System (PORTPASS) to monitor people in vehicles at borders through voice recognition. This system is currently being used at the U.S.-Canadian vehicle border crossing, and INS plans to use the same system at the U.S.-Mexican border crossing.

- The Federal Bureau of Prisons is using hand geometry units to monitor the movements of prisoners, staff, and visitors within certain federal prisons. Visitors must enroll upon entry and are given a magnetic stripe card containing information that points to their identifying information in a central database. They must carry this card with them at all times. Staff and inmates must also enroll in the system. Prison staff are enrolled to reduce the possibility of mistakenly identifying them as an inmate or for positive identification in the event of a disturbance. Prisoners are enrolled for access control to places such as the cafeteria, recreation lounges, and the hospital.

[2]INSPASS is used for citizens of 23 countries that are enrolled in the U.S. visa waiver program and visit the United States on business at least three times a year. In addition, diplomats, representatives to international organizations, and airline crews from the visa waiver program may voluntarily enroll in the INSPASS program.

- Federal law enforcement agencies such as the Federal Bureau of Investigation use an automated fingerprint identification system to more quickly search a database and match fingerprints of suspected criminals.

- Several federal agencies, including the Defense Advanced Research Projects Agency, Drug Enforcement Agency, Department of Defense, Department of Energy, Department of State, the Federal Bureau of Investigation, and the U.S. Mint, have acquired biometric devices for access control applications. The Department of Defense is researching biometrics as a means for enhancing computer network security. The Department of State is analyzing how biometrics might enable it to process passports and visas more efficiently.

- The General Services Administration (GSA) is working on implementing a system of "smart cards" for federal agencies.[3] In May 2000 GSA awarded governmentwide Smart Access Common ID contracts to five prime companies. These contracts, which are worth a maximum of $1.5 billion over a 10-year period, will provide the federal government with a wide range of smart card applications, including visual identification and authentication, and logical and physical access control. These applications may be supported by a variety of technologies, including biometrics, digital signatures, digitized photographs, and magnetic stripes. Currently, GSA is working with its five prime contractors to develop the smart card. According to GSA, various agencies have already expressed an interest in participating in the Smart Access Common ID contracts for both physical access to buildings and logical access to computer systems. These agencies include the Department of Defense, Department of State, Department of Justice, and Department of Veterans Affairs.

State and local governments have also implemented biometric technologies, primarily for use in the process of determining eligibility for public assistance benefits or entitlements. Pilot programs in several states report that they have experienced significant savings by requiring biometric verification for individuals applying for public benefits. For example, Los Angeles County in California implemented the Automated Fingerprint Image Reporting and Match (AFIRM) system to check the fingerprints of new welfare applicants against a database of prior claimants. The purpose of the system is to detect and deter fraudulent and duplicate benefit claims. California estimates that finger-imaging of welfare clients in just seven counties has saved about $86 million in the first 2 years of operation. The states of New York and Connecticut have implemented similar systems, reporting savings of $396 million and $15 million, respectively, in their first few years of operation. Moreover, such systems can be cost effective. For example, the state of Connecticut reports that it originally paid $5.2 million for its biometric identification systems and saved $9 million in the first year of operation. Eight states—Arizona, California, Connecticut, Illinois, Massachusetts, New Jersey, New York, and Texas—currently have biometric

[3]The development of smart cards for federal employees originated in recommendations from the National Performance Review and the Government Information Technology Services Board.

identification systems in place or in pilot mode. Other states considering such systems include Florida, Pennsylvania, and North Carolina.

- - - - -

I hope this information is helpful. We will make copies of this letter available to those who request it.

If you or your staff have any questions, please call me or Kay Brown, Assistant Director, at (202) 512-7215. Other staff who assisted in gathering this information include David Attianese, Yvette Banks, Ralph Block, and Jeremy Cox.

Sincerely yours,

Barbara D. Bovbjerg
Associate Director, Education,
Workforce, and Income Security Issues

(207106)